Office of the Chief Information Officer Enterprise Policy

CIO-090: Information Security Incident Response Policy

Effective Date: 3/5/2013
Last Revised: 3/19/2019
Last Reviewed: 3/19/2019

Policy Statement

This policy establishes controls related to the Commonwealth's Information Security Incident Response program. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions

Information Security Incident: A violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices.

Security Breach:

1. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises, or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) more individuals; or
2. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises, or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.

"Security breach" does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency, if the personal information is used for a purpose related to the agency and is not subject to unauthorized disclosure. KRS 61.931 (9)(a) and (b)

Policy

Agencies shall notify the Commonwealth Service Desk when they identify a potential security incident. When agencies believe a security incident is sensitive in nature, they shall contact the COT Security Office directly. The Office of the Chief Information Security Officer (CISO) shall review the incident and determine its appropriate response to the incident, ranging from an advisory role to leading the investigation.

The Commonwealth Office of Technology (COT) and affected agencies shall adhere to KRS 61.931 through KRS 61.934 and all federal, state, and local laws as well as COT policies to ensure appropriate reporting and remediation of a security breach. COT and agencies shall protect data and information about the breach in accordance with all applicable laws and policies.

COT, governmental agencies, and non-affiliated third parties that maintain or possess personal information, shall have reasonable security procedures and practices to protect and safeguard that information against security breaches in accordance with KRS 61.931 through KRS 61.934. COT, agencies, and non-affiliated third parties shall follow the procedures and practices of KRS

61.931 through KRS 61.934 for notification and reporting requirements by using the appropriate forms in 200 KAR 1:015 (Data Breach Notification Forms).

COT and agency personnel shall comply with all federal and state laws and policies for information disclosure to media or the public. COT will work closely with the management of affected agencies to ensure proper disclosure of security incident information. COT personnel and agencies shall not disclose agency data or information related to security incident responses unless required to do so by state or federal regulations.

Authority

KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government. KRS 42.724 gives the Office of the CISO the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities.

Applicability

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each agency must ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

The Office of the CISO is responsible for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle

The Office of the CISO will review this policy at least every two years.

References

- CIO-091 - Enterprise Information Security Program
- Commonwealth Service Desk (502) 564-7576
- COT Security Office (502) 564-1532
- Enterprise Architecture and Standards
- KRS 42.724 (3)(d), Commonwealth Office of Technology
- KRS 42.726, Roles, duties, and permissible activities for Commonwealth Office of Technology -- Duties of Archives and Records Commission and Department for Libraries and Archives not affected -- Annual report concerning security breaches.
- KRS 61.931, Definitions for KRS 61.931 to 61.934.

- KRS 61.932, Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties.
- KRS 61.933, Notification of personal information security breach - Investigation - Notice to affected individuals of result of investigation - Personal information not subject to requirements - Injunctive relief by Attorney General.
- KRS 61.934, Personal information security and breach investigation procedures and practices for legislative and judicial branches -- Personal information disposal or destruction procedures.
- 200 KAR 1:015, Data breach notification forms
- Finance Forms, Commonwealth Office of Technology, Data Breach Notification Forms:
    - FAC001 Determined Breach Notification Form
    - FAC002 Delay Notification Record
- NIST Special Publication 800-61, Computer Security Incident Handling Guide